STATE of ARIZONA

Government **I**nformation **T**echnology **A**gency	**Statewide** **STANDARD** **P800-S820 Rev 1.0**	**TITLE: Authentication and Directory Services** **Effective Date: April 5, 2004**

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to coordinate budget unit and State implementations associated with the identification and verification of information systems users who access resources or services through budget unit and State systems. Identification and verification provide the foundation for many other information security systems and services in the State.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches.
A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. STANDARD

Identification, authentication, and directory services are crucial for proper authorization to applications and systems, non-repudiation, and auditing capabilities for budget units. Without authentication, budget units have no assurance that access to resources and services is properly controlled and monitored.

To safeguard critical systems, applications, information and networks from unauthorized access or intrusion, budget units shall ensure identity and authentication of a user/customer before granting access to resources and services by implementing one or more of the following authentication methods:

- ***Authentication by Knowledge*** – Based on information only the user knows;
- ***Authentication by Ownership*** – Based on something only the user possesses;
- ***Authentication by Characteristic*** – Based on a user’s physical characteristic.

External connections to networks, in accordance with *Statewide Standard P800-S830, Network Security*, shall be routed through secure gateways, encrypted, and require strong authentication, such as challenge/response devices, one-time passwords, tokens, Kerberos, and smart cards, as well as the standard method of authentication required by the budget unit for internal connectivity (commonly referred to as multifactor authentication.)

Budget unit authentication methods shall be documented and maintained as part of, and in accordance with, *Statewide Standard P800-S810, Account Management*.

4.1. ACCESS TO RESOURCES AND SERVICES – shall be in accordance with *Statewide Standard P800-S885, IT Physical Security, Statewide Standard P800-S890, Personnel Security,* and *Statewide Standard P800-S810, Account Management*. Internal and external connectivity to networks to provide access to resources and services shall be in accordance with *Statewide Standard P800-S830, Network Security*.

4.2. DIRECTORY SERVICES - Lightweight Directory Access Protocol (LDAP) shall be used to provide access to directory and application services.

- LDAP is the lightweight version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
- As a widely accepted industry standard for access to directory information, LDAP supports multi-vendor interoperability by providing an open, extensible, vendor-independent, platform-independent, protocol standard.
- LDAP directories provide repositories for security-related data (e.g., userIDs, passwords, URLs, pointers, binary data, Public Key Certificates, etc.).
- The LDAP protocol directly supports various forms of strong security technology used to perform authentication, privacy, and data integrity services.
- The LDAP Version 3 proposal for Transport Layer Security (TLS) includes data encryption methods.
- LDAP supports the use of Directory Services Markup Language (DSML)v2 and Simple Object Access Protocol (SOAP) to allow LDAP directory information to be expressed in a common format and transmitted beyond the traditional firewall and into Internet-based applications.
- LDAP supports the use of the open, industry standard Java Naming and Directory Interface (JNDI) for directory access and support.
- LDAP supports the use of the Security Assertion Markup Language (SAML) standard as an authentication protocol that may be used between Web servers for federated affiliation.
- The Directory Enabled Networking (DEN) and Common Information Model (CIM) XML-based, industry-standard initiatives are being mapped into the LDAP directory structure. CIM is more comprehensive than the

Desktop Management Interface (DMI) model and can be used in conjunction with the Simple Network Management Protocol (SNMP).

- Future meta-directory services should be established with individual LDAP directory repositories and be accessible via standard LDAP protocols. Meta-directory service design should include obtaining an Object Identifier (OID) tree for the State from the Internet Assigned Numbers Authority (IANA) that can be used to uniquely identify attributes and object classes to facilitate the matching and coordination of information among individual LDAP implementations.

4.3. AUTHENTICATION BY KNOWLEDGE - User authentication shall be based on the presence of a userID associated with something only the user/customer knows and shall include the following:

4.3.1. Password – A secret series of characters that, by association with a userID, enables a user to access information, systems, applications, or networks. Budget units shall establish, implement, document, and communicate (in accordance with *Statewide Standard P800-S895, Security Training and Awareness*) criteria governing the following:

- A consistent treatment used throughout the budget unit (a mixture of upper/lower case characters, numbers, and special characters is recommended),
- Minimum password length and format,
- Maximum validity periods for passwords (passwords should be automatically set to expire),
- Password reuse limitations,
- Number of unsuccessful login attempts allowed, and
- Procedures for revoking and resetting passwords.

Use of passwords shall conform to the following requirements:

- Passwords shall be for individual users in order to maintain accountability. Generic, multi-user IDs should be eliminated
- Passwords shall be different from userIDs.
- Passwords shall be kept confidential.
- Passwords shall not be displayed when entered.
- Passwords shall not be transmitted in clear text format.
- Passwords shall not be kept on paper or stored in plain text format.
- Passwords shall be changed whenever there is a chance that the password or the system has been compromised.
- Passwords shall be changed periodically and not reused.
- Passwords shall not be included in a macro or function key to automate log-in processes.
- Vendor supplied passwords shall be changed immediately upon installation.
- Temporary passwords shall be changed on first use of the system.

- Passwords, along with hints and reminders, shall be stored in protected, encrypted files.
- Applicable devices and application systems shall maintain a password history file, where the capability exists, to prevent continual reuse of the same password for a valid userID.

4.3.2. Kerberos - A secure method for authenticating a request for a service in a computer network. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. It shall be based on symmetric cryptography, so the user's password does not actually pass through the network as plain text.

4.3.3. Personal Identification Number (PIN) - A character string used as a password to gain access to a system resource. PINs shall only be entered using a keypad and usually not sent across the network, to prevent interception. PINs may be used in conjunction with other types of authentication devices (i.e., a smart card).

4.4 AUTHENTICATION BY OWNERSHIP – User authentication shall be based on something only the user possesses, making it more secure than a knowledge-based system, and may include the following:

4.4.1 Hardware Based Challenge-Response – The server challenges the user to demonstrate that he/she possesses a specific token and knows the PIN or passphrase by combining them to generate a response that is valid, but only once. This includes but is not limited to:

- A small, handheld device, with or without a key pad, containing an LCD window or display interface – the device acts as the user's token.
- A smart card. An ISO 7816-compliant chip card with CPU and memory. Contact smart cards require PC/SC standard readers, based on ISO 7816, and supporting workstation software. Contactless smart cards require a Mifare architecture card reader based on ISO Standard 14443A.
- A Universal Serial Bus (USB) key. A device with CPU memory that plugs into a universal serial bus port on a workstation.
- A Bluetooth-enabled token with CPU and memory. Bluetooth is a short-range, 2.45GHz wireless connection protocol.

4.4.2 Symmetric-Key Cryptography - A cryptographic system in which the sender and receiver of a message share a single, common key used to encrypt and decrypt the message. (Reference *Statewide Standard P800-S850, Encryption Technologies*.)

4.4.3 Asymmetric-Key Cryptography - A cryptographic system that uses two keys, a *public key* known to everyone and a *private* or *secret key* known only to the recipient of the message. (Reference *Statewide Standard P800-S850, Encryption Technologies*.)

4.5 AUTHENTICATION BY CHARACTERISTIC – User authentication based on information about a person gathered by digitizing measurements of a physiological or behavioral characteristic has been categorized as an emerging technology. When used, implementations shall be based on open, industry standards, if available. Requirements may be issued for the following areas once the technology matures to the point of becoming strategic for the State:

4.5.1 Physiological characteristic such as:

- Fingerprint – any fingerprint imaging used shall conform to current Department of Public Safety (DPS) Fingerprint Imaging Bureau standards.
- Iris patterns.
- Retina patterns.
- Hand geometry.
- Face geometry.
- Palm print.

4.5.2 Behavioral characteristics such as:

- Voiceprint (speech patterns).
- Signature.
- Keystroke dynamics.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))),"State Agency Information."
6.3. A. R. S. § 41-1339 (A),"Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.8. A. R. S. § 41-3501, "Definitions."
6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.10. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.11. A. R. S. § 44-7041, "Governmental Electronic Records."

6.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
6.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration, Risk Management Section.”
6.14. Arizona Administrative Code, Title 2, Chapter 18, Government Information Technology Agency.”
6.15. Statewide Policy P100, Information Technology.
6.16. Statewide Policy P800, IT Security.
   6.16.1. Statewide Standard P800-S810, Account Management.
   6.16.2. Statewide Standard P800-S830, Network Security.
   6.16.3. Statewide Standard P800-S850, Encryption Technologies.
   6.16.4. Statewide Standard P800-S885, IT Physical Security.
   6.16.5. Statewide Standard P800-S890, Personnel Security.
6.17. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

None